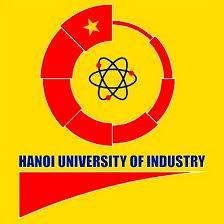
 **ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

---------------🙦 🕮 🙤--------------

****

**BÀI TẬP LỚN**

## MÔN: NGUYÊN LÝ HỆ ĐIỀU HÀNH

### ĐỀ TÀI

*Nghiên cứu tìm hiểu về Hệ thống bảo vệ trong hệ điều hành Linux*

**GIÁO VIÊN HƯỚNG DẪN : *Th.s* *Nguyễn Tuấn Tú***

**NHÓM THỰC HIỆN : 12**

**LỚP : IT6025.6(006)\_K15**

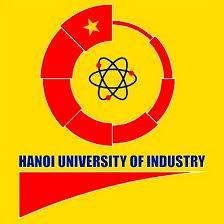
**HÀ NỘI 2022**

**--------------------------**

** ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**KHOA CÔNG NGHỆ THÔNG TIN**

---------------🙦 🕮 🙤--------------

****

**BÀI TẬP LỚN**

## MÔN: NGUYÊN LÝ HỆ ĐIỀU HÀNH

### ĐỀ TÀI

*Nghiên cứu tìm hiểu về Hệ thống bảo vệ trong hệ điều hành Linux*

**GIÁO VIÊN HƯỚNG DẪN : *Th.s* *Nguyễn Tuấn Tú***

**SINH VIÊN THỰC HIỆN :** **Lê Đức Bảo**

**Trần Tuấn Anh**

**Nguyễn Nhật Anh**

**Đặng Việt Anh**

**Nguyễn Trọng An**

**LỚP : IT6025.6(006)\_K15**

**HÀ NỘI 2022**

**--------------------------**

**MỤC LỤC**

Chương 1. Quan điểm cơ bản về hệ thống bảo mật, các kiểu tấn công mạng cơ bản……………………………………………………………………………….4

1.1. Quan điểm cơ bản về hệ thống bảo mật…………………………...4

1.2. Các kiểu tấn công mạng cơ bản……………………………………4

1. Denial of service (DoS) (Từ chối dịch vụ).......................................4
2. Intrusion (Xâm nhập).......................................................................4
3. Snooping (Rình mò).........................................................................5
4. Viruses, worms and Trojan Horses………………………………..5

Chương 2. Các bước ban đầu để thiết lập một hệ thống bảo mật trong Linux...6

2.1. Sử dụng chế độ bảo mật mặc định Kernel…………………………6

2.2. Ngắt kết nối tới các mạng không mong muốn……………………..8

2.3. Vô hiệu hóa các Service không sử dụng……………………….......9

2.4. Sử dụng TCP Wrapper....................................................................11

2.5. An toàn cho các giao dịch trên mạng…………………………......11

Chương 3. Linux Firewall…………………………………………………….12

3.1. Dùng công cụ dò tìm để khảo sát hệ thống……………………….12

3.2. Phát hiện sự xâm nhập qua mạng…………………………….......13

3.3. Kiểm tra khả năng bị xâm nhập…………………………………..14

3.4. Đối phó với hệ thống bị tấn công……………………………........15

Chương 4. Thiết lập tường lửa Iptables cho Linux……………………….......17

4.1. Giới thiệu về Iptables……………………………………………..17

4.2. Lập cấu hình Iptables cho máy chủ phục vụ web…………….......18

1. Thiết lập các tham số cho nhân……………………………...........18
2. Nạp các Module cần thiết cho Iptables……………………...........19
3. Nguyên tắc đặt luận là “Drop trước, Accept sau” ..........................19
4. Lọc ICMP vào và chặn ngập lụt PING……………………...........19
5. Reject quét cổng TCP và UDP……………………………….......19
6. Phát hiện quét cổng bằng Nmap…………………………….........19
7. Chặn ngập lụt SYN…………………………………………….....20

Lời nói đầu

Linux là một phần mềm hệ điều hành mã nguồn mở dựa trên hệ điều hành Unix và Linux cũng đang phát triển mạnh mẽ trên thế giới. Cùng với sự phát triển như vũ bảo của Windows và macOS thì Linux cũng đã có những bước đi chắc chắn trong thị trường công nghệ. Khác với Windows, Linux là hệ điều hành mã nguồn mở miễn phí, cho phép người dùng có thể sửa đổi mã nguồn và giao diện của nó. Chính vì vậy nó đã tạo ra sự bùng nổ trong tin học và ngày càng trở nên phổ biến. Mặc dù hệ điều hành này mang đến rất nhiều ưu điểm, tuy nhiên lại chưa được nhiều người Việt Nam biết đến và sử dụng nhiều như Windows hay macOS.

Bảo mật luôn là một vấn đề quyết định sự sống còn của Linux kể từ khi được phát triển rộng rãi và nhanh chóng cho đến nay, đặc biệt là trong các giao dịch quan trọng. Chính vì vậy trong bài tập lớn của nhóm, chúng em sẽ trình bày và tìm hiểu về những khái niệm cơ bản, những phương pháp đảm bảo an ninh cho máy tính sử dụng hệ điều hành Linux. Để hoàn thành bài tập lớn này chúng em đã tham khảo rất nhiều tài liệu về hệ điều hành Linux, trong đó chủ yếu là ở Running Linux, 4 Edition. Do thời gian làm bài tập còn hạn hẹp nên kết quả vẫn còn nhiều thiếu sót.

**Kính mong thầy có thể nhận xét và đóng góp ý kiến để nhóm chúng em có thể hoàn thiện hơn.**

**Em xin chân thành cảm ơn!**

**CHƯƠNG 1: QUAN ĐIỂM CƠ BẢN VỀ HỆ THỐNG BẢO MẬT, CÁC KIỂU TẤN CÔNG MẠNG CƠ BẢN.**

**1.1. Quan điểm cơ bản về hệ thống bảo mật**

* Có một quan điểm đúng đắn, công bằng về một hệ thống bảo mật đôi khi là rất khó. Phương tiện hướng tới các câu chuyện giật gân liên quan tới các hệ thống bảo mật, đặc biệt khi chúng bao gồm các công ty hoặc các viện nghiên cứu nổi tiếng. Mặt khác, quản lý bảo mật có thể là một thách thức về mặt kỹ thuật và là một công việc tốn khá nhiều thời gian. Rất nhiều người dùng Internet giữ cách nhìn rằng hệ thống của họ giữ những dữ liệu không có giá trị, bảo mật không nhiều. Số khác nỗ lực thật nhiều để bảo vệ hệ thống của họ khỏi việc sử dụng trái phép. Dù bạn nằm ở nhóm nào bạn cũng nên nhận thức rằng luôn có một sự rủi ro, nguy hiểm mà bạn sẽ trở thành nạn nhân của một cuộc tấn công bảo mật. Có rất nhiều lý do, chẳng hạn như tại sao ai đó thích tấn công vào hệ thống bảo mật của bạn. Giá trị của dữ liệu trên hệ thống của bạn chỉ là một trong số đó , chúng ta sẽ thảo luận về những cái khác tiếp theo trong phần sau.
* Hệ thống bảo mật truyền thống tập trung vào các hệ thống có thể truy cập thông qua một thiết bị cuối được kết nối hoặc một console. Trong lĩnh vực này nguy hiểm lớn nhất một cách tiêu biểu đến từ bên trong tổ chức sở hữu hệ thống, và dạng bảo mật tốt nhất là bảo vệ ở mức vật lí, nơi mà các console, các thiết cuối và host ở trong những “phòng” bị khóa. Thậm chí khi hệ thống máy tính được khởi động và kết nối vào mạng, truy cập vẫn rất hạn chế. Các mạng đang sử dụng thường đắt để truy cập, hoạc bị đóng mà không cho phép các kết nối tới host từ bất kỳ nơi nào.

**1.2. Các kiểu tấn công mạng cơ bản**

1. Denial of service (DoS) (Từ chối dịch vụ)

* Loại tấn công này làm giảm hoặc phá vỡ một dịch vụ hệ thống.

1. Intrusion (Xâm nhập)

* Loại tấn công này truy cập vào hệ thống bằng cách đoán các mật khẩu hoặc vạch trần các dịch vụ (service). Một khi kẻ xâm nhập đã truy cập được vào hệ thống, chúng có thể phá hỏng hoặc ăn cắp dữ liệu hay sử dụng hệ thống đích để tiến hành các cuộc tấn công khác trên host khác.

1. Snooping (Rình mò)

* Loại tấn công này bao gồm việc chặn dữ liệu của người dùng khác và nghe ngóng mật khẩu hoặc các thông tin nhạy cảm khác. Đôi khi loại tấn công này cũng bao gồm việc đổi dữ liệu. Snooping thường bao gồm việc nghe trộm trên các kết nối mạng, nhưng cũng có thể được thực hiện bằng cách vạch trần một hệ thống để chặn thư việc hoặc các lời gọi hệ thống mà mang các thông tin nhạy cảm (thông tin cá nhân, mật khẩu hay thông tin tín dụng…).

1. Viruses, worms, and Trojan Horses (Virus, sâu và Trojan Horses).

* Những loại tấn công này mỗi loại đều dựa vào một hành động của người sử dụng hoặc hệ thống để chạy các chương trình được cung cấp bởi kẻ tấn công. Các chương trình có thể được nhận trong một thư điện tử, hoặc từ một website, hay thậm chí ở trong một vài chương trình nhìn bề ngoài tưởng như vô hại được nhận ở đâu đó trên Internet và được cài vào máy cục bộ.
* Một cách chung, DoS tấn công chủ yếu bằng việc tự tạo ra một lượng lớn các yêu cầu (request) bất thường tới một dịch vụ được cung cấp bởi một hệ thống. Sự tấn công ồ ạt của hành động này có thể làm hệ thống host dốc hết bộ nhớ, sức mạnh tính toán hay băng thông mạng. Và kết quả, các yêu cầu xa hơn khác tới hệ thống bị từ chối, hoặc làm giảm hiệu suất của hệ thống xuống một mức không thể sử dụng được . Để cuộc tấn công có thể thực hiện được, kẻ tấn công phải tấn công một dịch vụ được thiết kế nghèo nàn hoặc có khả năng tự tạo ra một số lượng yêu cầu (request) vượt quá khả năng của một dịch vụ có thể đáp ứng.
* Một dạng quỷ quyệt của tấn công DoS là DDoS, từ chối dịch vụ phân tán. Trong dạng tấn công này, một số lượng lớn các máy tính làm nguyên nhân tạo ra các yêu cầu tới một dịch vụ. Điều này làm tăng sự nguy hại của một cuộc tấn công DoS theo hai hướng: bằng cách chôn vùi đích tấn công với một lượng lớn các yêu cầu, và bằng cách ẩn thủ phạm đằng sau hàng ngàn người tham gia không ý thức. Bằng việc sử dụng một lượng lớn các máy chủ từ đó tiến hành một cuộc tấn công cũng làm cho tấn công DDoS trở nên khó khăn để điều khiển hơn rất nhiều và không thể cứu chữa một khi nó đã xảy ra. Thậm chí những người mà không có liên quan gì với trạng thái của dữ liệu của họ cũng nên bảo vệ chính họ khỏi dạng tấn công này, để giảm thiểu tối đa mức nguy hiểm của việc trở thành kẻ tòng phạm không có ý thức trong một cuộc tấn công DDoS chống lại một ai đó khác.
* Dạng thứ hai của tấn công, đôi khi được gọi là cracking, là một trong những dạng mà hầu hết mọi người đều tiếp xúc trong vấn đề bảo mật. Các công ty và các tổ chức thường lưu trữ các thông tin nhạy cảm của họ trên một hệ thống máy tính có thể được nối mạng và truy cập với nhau. Một ví dụ chung nhất liên quan tới một người dùng Internet trung bình là lưu trữ thông tin chi tiết của thẻ tín dụng bởi các website. Nơi khuyến khích các cá nhân không lương thiện cố truy cập và ăn cắp, sử dụng sai mục đích, lạm dụng loại thông tin nhạy cảm này.
* Đôi khi các biện pháp mà được sử dụng để chống lại các truy cập bất hợp pháp hoặc làm sập các dịch vụ rất tài tình, khéo léo, nếu hợp đạo đức. Thiết kế một cơ chế xâm nhập thường yêu cầu một sự hiểu biết vững chắc về hệ thống đích để khám phá ra lỗ hổng. Thường thường, một khi một cơ chế xâm nhập đã được khám phá ra, nó được đóng gói trong dạng của một cái được gọi là rootkit, một tập hợp các chương trình hoặc kịch bản mà bất kì ai sở hữu chỉ với một chút hiểu biết cơ bản cũng có thể sử dụng để khai thác một lỗ hổng bảo mật. Khoảng rộng lớn chính yếu của các kẻ xâm nhập là được chạy bởi một "script kiddies" mà sử dụng những bộ xâm nhập được đóng gói trước mà không cần bất kì hiểu biết thực tế hệ thống mà chúng tấn công. Chúng ta sẽ thảo luận những cách khác nhau để bảo vệ hệ thống trong phần này.

**CHƯƠNG 2: CÁC BƯỚC BAN ĐẦU ĐỂ THIẾT LẬP MỘT HỆ THỐNG BẢO MẬT TRONG LINUX**

**2.1. Sử dụng chế độ bảo mật mặc định Kernel.**

Trước tiên ta cần đặt câu hỏi Kernel là gì? Khái niệm kernel ở đây nói đến những phần mềm, ứng dụng ở mức thấp (low-level) trong hệ thống, có khả năng thay đổi linh hoạt để phù hợp với phần cứng. Chúng tương tác với tất cả ứng dụng và hoạt động trong chế độ user mode, cho phép các quá trình khác – hay còn gọi là server, nhận thông tin từ các thành phần khác qua inter-process communication (IPC).

Trong Kernel của một số hệ thống Linux mới hiện giờ có cấu hình sẵn một vài Rules chuẩn với mục đích cung cấp những thông số căn bản nhất để cấu hình cho hệ thống dành cho những Admin không có nhiều kinh nghiệm về bảo mật hệ thống. Các File và thông số đó thường được chứa ở /proc/sys. Về căn bản giao thức IPV4, bên trong /proc/sys/net/ipv4 cung cấp các tính năng căn bản:

* *icmp\_echo\_ignore\_all*: Vô hiệu hoá tất cả các yêu phản hồi ICMP ECHO. Sử dụng tuỳ chọn này nếu như bạn không muốn hệ thống của mình trả lời các yêu cầu Ping.
* *icmp\_echo\_ignore\_broadcasts*: Vô hiệu hoá tất cả các yêu cầu phản hồi ICMP ECHO trên Broadcast và Multicast. Tùy chọn này được sử dụng để ngăn chặn nguy cơ hệ thống của bạn có thể bị lợi dụng khai thác cho những cuộc tấn công DDOS.
* *ip\_forward*: Cho phép hay không cho phép sự chuyển tiếp IP giữa các giao diện mạng trong hệ thống của bạn. Tuỳ chọn này được sử dụng khi bạn muốn Server của mình hoạt động như Router.
* *ip\_masq\_debug*: Kích hoạt hay vô hiệu hoá quá trình gỡ lỗi cho IP Masquerading
* *tcp\_syncookies*: Tùy chọn này được sử dụng để bảo vệ hệ thống của bạn chống các cuộc tấn công sử dụng kỹ thuật ngập SYN đã từng gây kinh hoàng một thời trên Internet.
* *rp\_filter:* Chứng thực và xác định địa chỉ IP nguồn hợp lệ. Tùy chọn này được sử dụng để bảo vệ hệ thống của bạn chống lại các cuộc tấn công giả mạo địa chỉ IP "IP Spoof".
* *secure\_redirects*: Chỉ chấp nhận chuyển tiếp những thông điệp ICMP cho những Gateway tin tưởng trong danh sách.
* *log\_martians*: Ghi lại những Package không được xử lý bở Kernel.
* *accept\_source\_route*: Xác định xem liệu có phải những Source Routed Packet được chấp nhận hay từ chối. Để an toàn bạn lên vô hiệu hoá tính năng này.

Trong hệ thống Redhat, ở /etc/sysctl.conf chứa thông tin về những thiết bị mặc định được xử lý ngay khi khởi động hệ thống, những thông số đó được đọc, điều khiển và thực thi bởi /usr/bin/sysctl.

Nếu bạn muốn vô hiệu hóa tính năng "ip\_forward" đơn giản bạn chỉ việc sử dụng lệnh: root@localhost# echo “0” > /proc/sys/net/ipv4/ip\_forward

Tương tự để kích hoạt tính năng nào bạn chỉ việc thay giá trị "0" bằng "1"…

**2.2. Ngắt kế nối tới các mạng không mong muốn.**

Bước đầu tiên trong việc bảo mật cho một hệ thống Linux là ngắt kết nối hay vô hiệu hóa tất cả các mạng ma và các dịch vụ mà bạn không cần. Một cách cơ bản, bất kì cổng mạng nào mà hệ thống đang chờ kết nối đều có thể nguy hiểm, bởi vì đó có thể là một sự khai thác bảo mật dựa vào một mạng mà sử dụng cổng đó. Cách nhanh nhất để tìm ra những cổng nào được mở là sử dụng netstat -an, như được chỉ ra dưới đây (tuy nhiên chúng ta sẽ bỏ đi một vài dòng): # netstat -an

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 0 0.0.0.0:7120 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:6000 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN

Ở đây chúng ta thấy rằng hệ thống này đang nghe ngóng cho những kết nối trên cổng 7120, 600 và 22. Nhìn vào /etc/services, hoặc sử dụng -p với lệnh netstat, có thể thường tiết lộ mạng ma nào đang giao tiếp với những cổng đó. Trong trường hợp này nó là X font server, X Window System server và SSH.

Nếu bạn nhìn thấy rất nhiều những cổng khác mở - cho những thứ như telnetd, sendmail...hãy tự hỏi bạn xem liệu bạn có thực sự cần những deamons đó chạy không. Qua thời gian, những vấn đề bảo mật sẽ càng bộc lộ, và trừ phi bạn có nhiều kinh nghiệm trong việc theo dõi tất cả những cập nhật bảo mật, nếu không hệ thống của bạn có thể bị tổn thương từ những cuộc tấn công. Bởi vậy, telnetd, ftpd, và rshd tất cả bảo gồm gửi các mật khẩu thông qua mạng Internet cho việc chứng thực, một giải pháp tốt hơn là sử dụng sshd, nó mã hóa dữ liệu và sử dụng một cơ chế chứng thực mạnh hơn. Thậm chí nếu bạn chưa bao giờ sử dụng telnetd thì để nó chạy trên hệ thống của bạn không phải là một ý kiến hay trong trường hợp một ai đó cố tìm một cách phá vỡ nó.

Ngắt các dịch vụ thường phải chỉnh sửa các file cấu hình tương ứng cho bản phân phối của bạn và khởi động lại hệ thống. Trên các hệ thống Red Hat, ví dụ, nhiều deamons được bắt đầu bằng các kịch bản trong thư mục /etc/rc.d/init.d

Đổi tên hoặc gỡ bỏ những file kịch bản đó có thể ngăn chặn deamons tương ứng từ lúc khởi động. Những deamon khác được khởi động bởi inetd hoặc xinetd trong việc trả lời các kết nối mạng; sửa những cấu hình của những hệ thống đó có thể giới hạn tập hợp các daemon chạy trên hệ thống của bạn.

Nếu bạn thực sự cần một dịch vụ chạy trên máy của bạn (chẳng hạn như X server), hãy tìm những cách để ngăn chặn các kết nối tới dịch vụ đó từ những máy chủ không mong muốn, chẳng hạn, sẽ là an toàn nhất để cho phép kết nối ssh chỉ từ những máy chủ tin tưởng, chẳng hạn chỉ từ những máy trong mạng nội bộ của bạn. Trong trường hợp của X server và X font server, cái mà chạy trên nhiều máy Linux, thường không có lí do để cho phép các kết nối tới những daemon từ bất kì thứ gì ngoài chính mạng cục bộ. Lọc các kết nối tới những daemon có thể được thực hiện bởi TCP wrapper hoặc IP filtering, chúng ta sẽ mô tả trong phần sau.

**2.3. Vô hiệu hóa các Service không sử dụng.**

Để tránh tình trạng có lỗ hổng bảo mật sau này bạn lên vô hiệu hoá và gỡ bỏ những chương trình, Service không dùng đến trên hệ thống của mình. Bạn có thể sử dụng các công cụ quản lý để hiển thị danh sách những gói phần mềm nào đã được cài đặt để thực hiện việc này (Redhat Package Manager - Linux )

Về cơ bản, các Service được định nghĩa hoạt động bởi inetd (trên một số hệ thống Linux mới nó có thể là xinetd). Nội dung Service được định nghĩa hoạt động bởi inetd được chứa ở /etc/inetd.conf. Mỗi Service được định nghĩa đằng sau ký tự "#"...Bạn có thể vô hiệu hóa Service không sử dụng.

Thư mục /etc/rc\*.d và /etc/rc.d/rc\* là nơi chứa các Shell Script và các thông số để điều khiển sự thực hiện của Network và Service trong suốt thời gian nó hoạt động. Bạn có thể xoá bỏ hết những thứ liên quan đến những Service mà bạn không cần sử dụng. Đối với hệ thống Redhat, SuSE, Mandrake...bạn có thể sử dụng lệnh:

root@localhost#chkconfig --list

root@localhost#chkconfig --del <name>

Để hiển thị những Service nào đang hoạt động và xoá bỏ Service nào mà bạn muốn. Bạn muốn kiểm tra xem Service nào đó thực sự đã được gỡ bỏ khỏi hệ thống chưa?

/bin/netstat -a -p --inet

Trên Redhat, SuSE, Mandrake...chương trình được sử dụng để quản lý các gói phần mềm là /bin/rpm (Redhat Package Manager). Trên Debian là /usr/bin/dpkg (Debian Package ). Dưới đây là một số dòng lệnh cơ bản được dùng để quản lý các gói phần mềm. Dòng đầu sẽ là rpm và dòng thứ hai sẽ là dpkg:

**Gỡ bỏ một gói phần mềm:**

root@localhost# rpm -e <package-name>

root@localhost# dpkg -r <package-name>

**Liệt kê danh sách những gói đã được cài đặt:**

root@localhost# rpm -qvl <package-name.rpm>

root@localhost# dpkg -c <package-name.deb>

**Liệt kê danh sách những gói đã được cài đặt với thông tin chi tiết cho mỗi gói:**

root@localhost# rpm -qvia

root@localhost# dpkg -l

**Liệt kê thông tin chính xác các File của gói đã được chỉ định:**

root@localhost# rpm -qvpl <package-name.rpm>

root@localhost# dpkg -c <package-name.deb>

**Hiển thị thông tin về một gói phần mềm:**

root@localhost# rpm -qpi <package-name.rpm>

root@localhost# dpkg -I <package-name.deb>

**Kiểm tra tính toàn vẹn cho một gói phần mềm:**

root@localhost# rpm -Va

root@localhost# debsums -a

**Cài đặt một gói phần mềm mới:**

root@localhost# rpm -Uvh <package-name.rpm>

root@localhost# dpkg -i <package-name.deb>

**2.4. Sử dụng TCP Wrapper.**

Trước khi Server FTP được chạy. Đầu tiên tcpd sẽ xác định những địa chỉ nguồn được cho phép, các kết nối sẽ được gửi đến Syslog để đối chiếu sau này. Nếu bạn muốn vô hiệu hoá tất cả các Service, bạn chỉ việc thêm dòng sau vào File:

/etc/host.denny ALL:ALL

Để gửi E-mail đến nhà quản trị hệ thống và thông báo những lần kết nối bị thất bại, bạn thêm vào các dòng sau:

ALL: ALL: /bin/mail \

-s “%s connection attempt from %c” admin@mydom.com

Nếu bạn muốn cho phép những địa chỉ tin cậy chạy những dịch vụ mà họ được phép, bạn hãy chỉnh sửa nội dung File /etc/host.allow

sshd: magneto.mydom.com, juggernaut.mydom.com

in.ftpd: 192.168.1.

Để đảm bảo an toàn bạn lên kiểm soát và điều khiển quá trình truy nhập một cách cẩn thận hơn. Sử dụng tcpdchk để kiểm tra sự truy nhập File, sử dụng Syslog để ghi lại những lần đăng nhập thất bại...Bạn lên điều khiển sự truy nhập cho hệ thống của mình theo nguyên tắc:

Sự truy cập chỉ được thực hiện khi Client/Deadmon có địa chỉ phù hợp với nội dung được cho phép trong /etc/hosts.allow

**2.5. An toàn cho các giao dịch trên mạng.**

Có rất nhiều dịch vụ mạng truyền thống giao tiếp thông qua giao thức văn bản không mã hoá, như TELNET, FTP, RLOGIN, HTTP, POP3. Trong các giao dịch giữa người dùng với máy chủ, tất cả các thông tin dạng gói được truyền qua mạng dưới hình thức văn bản không được mã hoá. Các gói tin này có thể dễ dàng bị chặn và sao chép ở một điểm nào đó trên đường đi. Việc giải mã các gói tin này rất dễ dàng, cho phép lấy được các thông tin như tên người dùng, mật khẩu và các thông tin quan trọng khác. Việc sử dụng các giao dịch mạng được mã hoá khiến cho việc giải mã thông tin trở nên khó hơn và giúp bạn giữ an toàn các thông tin quan trọng. Các kỹ thuật thông dụng hiện nay là IPSec, SSL, TLS, SASL và PKI. Quản trị từ xa là một tính năng hấp dẫn của các hệ thống UNIX. Người quản trị mạng có thể dễ dàng truy nhập vào hệ thống từ bất kỳ nơi nào trên mạng thông qua các giao thức thông dụng như telnet, rlogin. Một số công cụ quản trị từ xa được sử dụng rộng rãi như linuxconf, webmin cũng dùng giao thức không mã hoá. Việc thay thế tất cả các dịch vụ mạng dùng giao thức không mã hoá bằng giao thức có mã hoá là rất khó. Tuy nhiên, bạn nên cung cấp việc truy cập các dịch vụ truyền thống như HTTP/POP3 thông qua SSL, cũng như thay thế các dịch vụ telnet, rlogin bằng SSH.

**CHƯƠNG 3 : LINUX FIREWALL**

**3.1. Dùng công cụ dò tìm để khảo sát hệ thống.**

* Thâm nhập vào một hệ thống bất kỳ nào cũng cần có sự chuẩn bị. Hacker phải xác định ra máy đích và tìm xem những port nào đang mở trước khi hệ thống có thể bị xâm phạm. Quá trình này thường được thực hiện bởi các công cụ dò tìm (scanning tool), kỹ thuật chính để tìm ra máy đích và các port đang mở trên đó. Dò tìm là bước đầu tiên hacker sẽ sử dụng trước khi thực hiện tấn công. Bằng cách sử dụng các công cụ dò tìm như Nmap, hacker có thể rà khắp các mạng để tìm ra các máy đích có thể bị tấn công. Một khi xác định được máy này, kẻ xâm nhập có thể dò tìm các port đang lắng nghe. Nmap cũng sử dụng một số kỹ thuật cho phép xác định khá chính xác loại máy đang kiểm tra.
* Bằng cách sử dụng những công cụ của chính các hacker thường dùng, người quản trị hệ thống có thể nhìn vào hệ thống của mình từ góc độ của hacker và giúp tăng cường tính an toàn của hệ thống. Có rất nhiều công cụ dò tìm có thể sử dụng như: Nmap, strobe, sscan, SATAN,...

**Nmap**

* Là chữ viết tắt của “Network exploration tool and security scanner”. Đây là chương trình quét hàng đầu với tốc độ cực nhanh và cực mạnh. Nó có thể quét trên mạng diện rộng và đặc biệt tốt với mạng đơn lẻ. Nmap giúp bạn xem những dịch vụ nào đang chạy trên server (services/ports:webserver, ftpserver, pop3,...), server đang dùng hệ điều hành gì, loại tường lửa mà server sử dụng,... và rất nhiều tính năng khác. Nói chung Nmap hỗ trợ hầu hết các kỹ thuật quét như: ICMP (ping sweep), IP protocol, Null scan, TCP SYN (half open), … Nmap được đánh giá là công cụ hàng đầu của các Hacker cũng như các nhà quản trị mạng trên thế giới. Quét an toàn Nmap là một trong số công cụ quét an toàn được sử dụng rộng rãi nhất sẵn có. Nmap là một cổng quét mà chống lại các nhân tố, các cách khác tàn phá đến mạng của bạn. Nó có thể phát sinh ra nhiều kiểu gói mà thăm dò các ngăn xếp TCP/IP trên những hệ thống của bạn.
* Nmap có thể phát sinh ra một danh sách của những cổng mở dịch vụ trên hệ thống của bạn, thâm nhập firewalls và cung cấp những tin quấy rầy, không tin cậy đang chạy trên host của bạn. Nmap security có sẵn tại: http:/[www.insecure.org](http://www.insecure.org) .

Tuy nhiên, sử dụng các công cụ này không thể thay thế cho một người quản trị có kiến thức. Bởi vì việc dò tìm thường dự báo một cuộc tấn công, các site nên ưu tiên cho việc theo dõi chúng. Với các công cụ dò tìm, các nhà quản trị hệ thống của mình.

**3.2. Phát hiện sự xâm nhập qua mạng.**

* Nếu hệ thống của bạn có kết nối vào internet, bạn có thể trở thành một mục tiêu bị dò tìm các lỗ hổng về bảo mật. Mặc dù hệ thống của bạn có ghi nhận điều này hay không thì vẫn không đủ để xác định và phát hiện việc dò tìm này. Một vấn đề cần quan tâm khác là các cuộc tấn công gây ngừng dịch vụ (Denial of Services - DoS), làm thế nào ngăn ngừa, phát hiện và đối phó với chúng nếu bạn không muốn hệ thống của bạn nhưng trệ.
* Hệ thống phát hiện xâm nhập qua mạng (Network Intrusion Detection System - NIDS) theo dõi các thông tin truyền trên mạng và phát hiện nếu có hacker đang cố xâm nhập vào hệ thống (hoặc gây ra một vụ tấn công DoS). Một ví dụ điển hình là hệ thống theo dõi số lượng lớn các yêu cầu kết nối TCP đến nhiều port trên một máy nào đó, do vậy có thể phát hiện ra nếu có ai đó đang thử một tác vụ dò tìm TCP port. Một NIDS có thể chạy trên máy cần theo dõi hoặc trên một máy độc lập theo dõi toàn bộ thông tin trên mạng.
* Các công cụ có thể được kết hợp để tạo một hệ thống phát hiện xâm nhập qua mạng. Chẳng hạn dùng tcpwrapper để điều khiển, ghi nhận các dịch vụ đã được đăng ký. Các chương trình phân tích nhật ký hệ thống, như swatch, có thể dùng để xác định các tác vụ dò tìm trên hệ thống. Và điều quan trọng nhất là các công cụ có thể phân tích các thông tin trên mạng để phát hiện các tấn công DoS hoặc đánh cắp thông tin như tcpdump, ethereal, ngrep, NFR (Network Flight Recorder), PortSentry, Sentinel, Snort,...
* Khi hiện thực một hệ thống phát hiện xâm nhập qua mạng bạn cần phải lưu tâm đến hiệu suất của hệ thống cũng như các chính sách bảo đảm sự riêng tư.

**3.3. Kiểm tra khả năng bị xâm nhập.**

* Kiểm tra khả năng bị xâm nhập liên quan đến việc xác định và sắp xếp lỗ hổng an ninh trong hệ thống bằng cách dùng một số công cụ kiểm tra. Nhiều công cụ kiểm tra cũng có khả năng khai thác một số lỗ hổng tìm thất để làm rõ quá trình thâm nhập trái phép sẽ được thực hiện như thế nào. Ví dụ, một lỗi tràn bộ đệm của chương trình phục vụ dịch FTP có thể dẫn đến việc thâm nhập vòa hệ thống với quyền “root”. Nếu người quản trị mạng có kiến thwucs về kiểm tra khả năng bị xâm nhập trước khi nó xảy ra, họ có thể tiến hành các tác vụ để nâng cao mức độ an ninh của hệ thống mạng.
* Có rất nhiều các công cụ mạng mà bạn có thể sử dụng trong việc kiểm tra khả năng bị xâm nhập. Hầu hết các quá trình kiểm tra đều dùng ít nhất một công cụ tự động phân tích các lỗ hổng an ninh. Các công cụ này thăm dò hệ thống để xác định các dịch vụ hiện có. Thông tin lấy từ các dịch vụ này sẽ được so sánh với cơ sở dữ liệu các lỗ hổng an ninh đã được tìm thấy trước đó.
* Các công cụ thường được sử dụng để thực hiện các kiểm tra loại này là ISS Scanner, Cybercop, Retina, Nessus, Cgiscan, CIS,...
* Kiểm tra khả năng bị xâm nhập cần được thực hiện bởi những người có trách nhiệm một cách cẩn thận. Sự thiếu kiến thức và sử dụng sai cách có thể sẽ dẫn đến hậu quả nghiêm trọng không thể lường trước được.

**3.4 Đối phó khi hệ thống bị tấn công**

* Gần đây, một loạt các vụ tấn công nhắm vào các site của những công ty lớn như Yahoo!, Buy.com, EBay, Amazon và CNN Interactive gây ra những thiệt hại vô cùng nghiêm trọng. Những tấn công này là dạng tấn công gây ngừng dịch vụ “Denial-Of-Service” mà được thiết kế để làm ngưng hoạt động của một mạng máy tính hay một website bằng cách gửi liên tục với số lượng lớn các dữ liệu tới mục tiêu tấn công khiến cho hệ thống bị tấn công bị ngừng hoạt động, điều này tương tự như hàng trăm người cùng gọi không ngừng tới 1 số điện thoại khiến nó liên tục bị bận.
* Trong khi không thể nào tránh được mọi nguy hiểm từ các cuộc tấn công, chúng tôi khuyên bạn một số bước mà bạn nên theo khi bạn phát hiện ra rằng hệ thống của bạn bị tấn công. Chúng tôi cũng đưa ra một số cách để giúp bạn bảo đảm tính hiệu quả của hệ thống an ninh và những bước bạn nên làm để giảm rủi ro và có thể đối phó với những cuộc tấn công.

***Những bước nên làm khi hệ thống bị tấn công:***

* Tập hợp 1 nhóm để đối phó với sự tấn công.
* Nhóm này phải bao gồm những nhân viên kinh nghiệm, những người mà có thể giúp hình thành một kế hoạch hành động đối phó với sự tấn công.
* Dựa theo chính sách và các quy trình thực hiện về an ninh của công ty, sử dụng các bước thích hợp khi thông báo cho mọi người hay tổ chức về cuộc tấn công.
* Tìm sự giúp đỡ từ nhà cung cấp dịch vụ Internet và cơ quan phụ trách về an ninh máy tính.
* Liên hệ nhà cung cấp dịch vụ Internet của bạn để thông báo về cuộc tấn công. Có thể nhà cung cấp dịch vụ Internet của bạn sẽ chặn dừng được cuộc tấn công.
* Liên hệ cơ quan phụ trách về an ninh máy tính để thông báo về cuộc tấn công.
* Tạm thời dùng phương thức truyền thông khác (chẳng hạn như qua điện thoại) khi trao đổi thông tin để đảm bảo rằng kẻ xâm nhập không thể chặn và lấy được thông tin.
* Ghi lại tất cả các hoạt động của bạn (chẳng hạn như gọi điện thoại, thay đổi file,...)
* Theo dõi các hệ thống quan trọng trong quá trình bị tấn công bằng các phần mềm hay dịch vụ phát hiện sự xâm nhập (intrusion detection software/services). Điều này có thể giúp làm giảm nhẹ sự tấn công cũng như phát hiện những dấu hiệu của sự tấn công thực sự hay chỉ là sự quấy rối nhằm đánh lạc hướng sự chú ý của bạn (chẳng hạn một tấn công DoS với dụng ý làm sao nhãng sự chú ý của bạn trong khi thực sự đây là một cuộc tấn công nhằm xâm nhập vào hệ thống của bạn). Sao chép lại tất cả các files mà kẻ xâm nhập để lại hay thay đổi (như những đoạn mã chương tình, log file,...)
* Liên hệ nhà nước chức trách để báo cáo về vụ tấn công.

***Những bước nên làm để giảm rủi ro và đối phó với sự tấn công trong tương lai:***

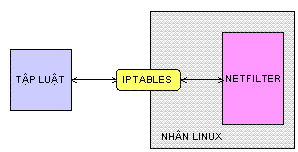
* Xây dựng và trao quyền cho nhóm đối phó với sự tấn công.
* Thi hành kiểm tra an ninh và đánh giá mức độ rủi ro của hệ thống.
* Cài đặt các phần mềm an toàn hệ thống phù hợp để giảm bớt rủi ro
* Nâng cao khả năng của mình về an toàn máy tính.
* Các bước kiểm tra để giúp bạn bảo đảm tính hiệu quả của hệ thống an ninh.
* Kiểm tra hệ thống an ninh mới cài đặt: chắc chắn tính đúng đắn của chính sách an ninh hiện có và cấu hình chuẩn của hệ thống.
* Kiểm tra tự động thường xuyên: để khám phá sự “viếng thăm” của những hacker hay những hành động sai trái của nhân viên trong công ty.
* Kiểm tra ngẫu nhiên: để kiểm tra chính sách an ninh và những tiêu chuẩn, hoặc kiểm tra sự hiện hữu của những lỗ hổng đã được phát hiện (chẳng hạn những lỗi được thông báo từ nhà cung cấp phần mềm)
* Kiểm tra hằng đêm những file quan trọng: để đánh giá sự toàn vẹn của những file và cơ sở dữ liệu quan trọng.
* Kiểm tra các tài khoản người dùng: để phát hiện các tài khoản không sử dụng, không tồn tại,...
* Kiểm tra định kỳ để xác định trạng thái hiện tại của hệ thống an ninh của bạn.

**CHƯƠNG 4: THIẾT LẬP TƯỜNG LỬA IPTABLES CHO LINUX**

**4.1. Giới thiệu về Iptables**

**Khái niệm**:

* Iptables là một tường lửa ứng dụng lọc gói dữ liệu rất mạnh, miễn phí và có sẵn trên linux… Iptables gồm 2 phần là Netfilter ở trong nhân linux và Iptables nằm ngoài nhân. Iptables chịu trách nhiệm giao tiếp giữa người dùng và Netfilter để đẩy các luật của người dùng vào cho Netfilter xử lý. Netfilter tiến hành lọc các gói dữ liệu ở mức IP. Netfilter làm việc trực tiếp trong nhân, nhanh và không làm giảm tốc độ của hệ thống



**Cấu trúc của một Iptables:**

* Iptables được chia làm 4 bảng: bảng filter dùng để lọc gói dữ liệu, bảng NAT dùng để thao tác với các gói dữ liệu được NAT nguồn hay NAT đích, bảng mangle dùng để thay đổi các thông số trong gói IP, bảng conntrack dùng để theo dõi các kết nối
* Mỗi bảng được chia thành nhiều mắt xích (chain). Chain gồm nhiều luật (rule) để thao tác với các gói dữ liệu. Rule có thể là ACCEPT (chấp nhận gói dữ liệu), DROP (thả gói dữ liệu), REJECT (loại bỏ gói) hoặc tham chiếu (reference) đến một chain khác

**4.2. Lập cấu hình Iptables cho máy chủ phục vụ web**

Giả sử máy chủ phục vụ web kết nối mạng trực tiếp vào internet qua card mạng eth0, địa chỉ IP là 1.2.3.4. Cần lập tường lửa cho Iptables đáp ứng các yêu cầu sau:

* Cổng TCP 80 (chạy apache) mở cho mọi người truy cập web
* Cổng 21 (chạy proftpd) chỉ mở cho webmaster (dùng để upload file lên public\_html)
* Cổng 22 (chạy openssh) chỉ mở cho admin (cung cấp shell ‘root’ cho admin để nâng cấp và patch lỗi cho server khi cần)
* Cổng UDP 53 (chạy tinydns) để phục vụ tên miền (đây chỉ là ví dụ)
* Chỉ chấp nhận ICMP PING tới với code=0x08, các loại packet còn lại đều bị từ chối

Bước 1: Thiết lập các tham số cho nhân

*echo 1 > /proc/sys/net/ipv4/tcp\_syncookies*

*echo 10 > /proc/sys/net/ipv4/tcp\_fin\_timeout*

*echo 1800 > /proc/sys/ipv4/tcp\_keepalive\_time*

*echo 0 > /proc/sys/net/ipv4/tcp\_window\_scaling*

*echo 0 > /proc/sys/net/ipv4/tcp\_sack*

*echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts*

*echo 0 > /proc/sys/net/ipv4/conf/eth0/accept\_source\_route*

tcp\_syncookies=1 bật chức năng chống DoS SYN qua syncookie của Linux

tcp\_fin\_timeout=10 đặt thời gian timeout cho quá trình đóng kết nối TCP là 10 giây

tcp\_keepalive\_time=1800 đặt thời gian giữ kết nối TCP là 1800 giây

tcp\_window\_scaling=0 tắt chế độ window scaling

tcp\_sack=0 tắt chế độ TCP SACK

icmp\_echo\_ignore\_broadcasts=1 không trả lời các gói tin ICMP boardcast để phòng tránh tấn công Smurf

accept\_source\_route=0 tắt tính năng source routing trên toàn bộ các card mạng hiện tại

Bước 2: Nạp các module cần thiết cho Iptables

Để sử dụng Iptables, bạn cần phải nạp trước các module cần thiết. Ví dụ nếu bạn muốn dùng chức năng LOG trong Iptables, bạn phải nạp module ipt\_LOG vào trước bằng lệnh #modprobe ipt\_LOG

*MODULE=”ip\_tables iptable\_filter ipt\_LOG ipt\_limit ipt\_REJECT ipt\_state for i in $MODULES; do*

*/sbin/modprobe $MODULES*

*done*

Bước 3: Nguyên tắc đặt luật là ”DROP trước, ACCEPT sau”

Đây là nguyên tắc mà bạn nên tuân theo. Đầu tiên hãy đóng hết các cổng, sau đó mở dần các cổng cần thiết. Các này giúp tránh được sai sót trong khi đặt luật cho Iptables

Bước 4: Lọc ICMP vào và chặn ngập lụt PING

LOG của Iptables sẽ được ghi vào file /var/log/firewall.log. Bạn phải sửa lại cấu hình cho SYSLOG như sau:

# vi /etc/syslog.conf

kern.=debug /var/log/firewall.log

# /etc/rc.d/init.d/syslog restart

Đối với các gói ICMP, chúng ta sẽ đẩy qua chain CHECK\_PINGFLOOD để kiểm tra xem hiện tại đang bị ngập lụt PING hay không, sau đó mới cho phép gói vào. Nếu đang bị ngập lụt PING, module LOG sẽ tiến hành ghi nhật kí ở mức giới hạn –limit $LOG\_LIMIT và --limit-burst $LOG\_LIMIT\_BURST, các gói PING ngập lụt sẽ bị thả hết

Bước 5: REJECT quét cổng TCP và UDP

Ở đây bạn tạo sẵn chain REJECT quét cổng, chúng ta sẽ đẩy vào chain INPUT sau. Đối với gói TCP, chúng ta REJECT bằng gói TCP với cờ SYN=1 còn đối với gói UDP chúng ta sẽ REJECT bằng gói ICMP ‘port-unreachable’

Bước 6: Quét cổng bằng NMAP

Đối với các gói TCP đến eth0 mở kết nối nhưng không đặt SYN=1 chúng ta sẽ chuyển sang chain DETECT\_NMAP. Đây là những gói không hợp lệ và hầu như là quét cổng bằng NMAP hoặc kênh ngầm. Chain DETECT\_NMAP sẽ phát hiện ra hầu hết các kiểu quét của NMAP và tiến hành ghi nhật ký ở mức --limit $LOG\_LIMIT và --limit-burst $LOG\_LIMIT\_BURST. Ví dụ để kiểm tra quét XMAS, bạn dùng tùy chọn --tcp-flags ALL FIN,URG,PSH nghĩa là 3 cờ FIN, URG và PSH được bật, các cờ khác đều bị tắt, Các gói qua chain DETECT\_MAP đều bị tắt

Bước 7: Chặn ngập lụt SYN

Gói mở TCP với cờ SYN được set 1 là hợp lệ nhưng không ngoại trừ khả năng là các gói SYN dùng để ngập lụt. Vì vậy, ở đây bạn đẩy các gói SYN còn lại qua chain CHECK\_SYNFLOOD để kiểm tra ngập lụt SYN

Bước 8: Giới hạn truy nhập SSH cho admin

Bước 9: Giới hạn FTP cho webmaster

Bước 10: Lọc TCP vào

Bước 11: Lọc UDP vào và chặn ngập lụt UDP

**TỔNG KẾT**

Với đề tài: Nghiên cứu tìm hiểu về hệ thống bảo vệ trong hệ điều hành Linux. Chúng em tìm hiểu về 3 phần lớn đó là:

**Phần 1: Quan điểm cơ bản về hệ thống bảo mật, các kiểu tấn công mạng cơ bản**

**Phần 2: Các bước ban đầu để thiết lập một hệ thống bảo mật trong Linux**

**Phần 3: Linux Firewall**

* Trong quá trình làm và hoàn thiện bài tập lớn, nhóm chúng em đã học hỏi được rất nhiều về hệ điều hành Linux. Chúng em chủ yếu dùng Windows nên có rất nhiều thắc mắc và khó khăn trong quá trình thực hiện. Tuy nhiên với sự giúp đỡ nhiệt tình của thầy cô hướng dẫn nên chúng em đã nỗ lực cùng nhau tìm hiểu để hoàn thiện đề tài này. Dù còn nhiều thiếu sót song đây cũng là một quá trình cố gắng để đạt được thành quả như ngày hôm nay.

- Cùng với những kiến thức đã học tại trường và những kiến thức tìm hiểu bên ngoài nhóm chúng em đã hoàn thành đề tài. Tuy nhiên với kiến thức của chúng em vẫn còn nhiều thiếu sót trong khi làm, chúng em hy vọng sẽ nhận được những góp ý, bổ sung tích cực từ thầy cô và các bạn để đề tài chúng em hoàn thiện hơn. Qua đây chúng em xin gửi lời cảm ơn chân thành đến thầy đã tận tình giúp đỡ, hướng dẫn chúng em hoàn thành tốt đề tài này.